CONTACT **General:** 1.877.388.4373 **Support:** 1.888.638.6771 **Sales:** 1.855.388.1260

Acceptable Use Policy

Updated: March 1, 2017

CenturyLink ("CenturyLink") has created this Acceptable Use Policy, hereinafter referred to as the AUP, with which you (the "Customer") must comply when using services and products (collectively, "Services") made available by CenturyLink to Customer, including, without limitation, on CenturyLink's website, www.CenturyLink.com ("Website").

Acceptable Use Policy. **By using the Services and the Website, Customer is accepting the policies described in this AUP. If Customer does not agree to the terms of this AUP, Customer must not use the Services or the Website. The AUP is not an all-inclusive or exhaustive list of prohibited activities, and CenturyLink reserves the right to modify or amend the terms of this AUP from time to time without notice. Customer's continued use of the Services and the Website following the posting of changes to this policy will mean that Customer accepts those changes. If CenturyLink intends to apply the modifications or amendments to this AUP retroactively, CenturyLink will provide Customer with notice of the modifications or amendments.**

Compliance with Law: Customer shall not post, transmit, re-transmit or store material on or through any of CenturyLink's Services which, in the sole judgment of CenturyLink (i) is in violation of any local, state, federal or non-United States law or regulation, (ii) is threatening, obscene, indecent, defamatory or otherwise could adversely affect any individual, group or entity, or (iii) violates the rights of any person, including rights protected by copyright, trade secret, patent or other intellectual property or similar laws or regulations including, but not limited to, the installation or distribution of "pirated" or other software products

Platform Services (/legal/)
Agreement (/legal/centurylink-cloud/agreement/)
Service Guide (/legal/centurylink-cloud/serviceguide/)
Supplemental Terms (/legal/centurylink-cloud/supplementalterms/)
Privacy Policy (/legal/centurylink-cloud/privacy/)
SLA (/legal/centurylink-cloud/sla/)
Digital Millennium Copyright Act (/legal/centurylink-cloud/dmca/)

that are not appropriately licensed for use by Customer. Customer shall be responsible for determining what laws or regulations are applicable to its use of the Services.

Customer Security Obligation: Customer must use reasonable care in keeping its software on the CenturyLink's servers up-to-date and patched with the latest security updates. A compromised server creating network interference may result in immediate shutdown of the server. If the compromised server is not causing network interference, CenturyLink staff will work with Customer to resolve the issue and if it cannot be resolved in a timely manner the compromised server will be disconnected from the network. No service credits will be issued for outages resulting from disconnection due to breached server security. Customer is solely responsible for any breaches of security under Customer control affecting servers. If Customer intentionally creates a security breach, the cost to resolve any damage to Customer's server or other servers will be charged directly to Customer. The labor used to resolve such damage is categorized as Emergency Security Breach Recovery and is currently charged at $300 USD per hour.

System and Network Security: Customer shall not violate CenturyLink's system or network security, and any such violations may result in criminal and civil liability. CenturyLink investigates all incidents involving such violations and will cooperate with law enforcement if criminal violation is suspected. Examples of system or network security violations include, without limitation, the following:

- Introduction into the network or server and/or distribution of malicious programs including viruses, worms, Trojan Horses, root kits, password crackers, adware, and key stroke capture programs (and other executables intended to inflict harm such as root kits, password crackers, adware, key stroke capture programs and other programs).
- Causing security breaches or disruptions of Internet communication and/or connectivity. Security breaches include, but are not limited to, accessing data, accounts or systems without authorization or logging into a server or account that the Customer is not expressly authorized to access. Disruptions include port scans, flood pings, email-bombing, packet spoofing, IP spoofing and forged routing information.

- Circumventing user authentication or security of any host, network or account.
- Unauthorized access, alteration, destruction, or any attempt thereof, of any information of any CenturyLink customers or end-users by any means or device, including the use of sudo or other privileged operating system commands.
- Knowingly engaging in any activities designed to harass, or that will cause a denial-of-service (e.g., synchronized number sequence attacks) to any other user whether on the CenturyLink network or on another provider's network.
- Using CenturyLink's Services to interfere with the use of the CenturyLink's network by other customers or authorized users.
- Using any program script/command, or sending messages of any kind, designed to interfere with or to disable, a user's terminal session, via any means, locally or via the Internet.
- Obtaining or attempting to obtain service by any means or device with intent to avoid payment.
- Accessing or attempting to access Customer account or other CenturyLink services after Customer (or CenturyLink) has terminated Customer's account.
- Failing to comply with the CenturyLink's procedure relating to the activities of customers on the CenturyLink's premises. Violators of this policy are responsible, without limitations, for the cost of labor to correct all damage done to the operation of the network and business operations supported by the network. Such labor is categorized as Emergency Security Breach Recovery and is currently charged at US $300 per hour required. Network interference by any Customers that may cause or is currently causing network interference will be disconnected immediately.
- Phishing: Any activity associated with Phishing or systems designed to collect personal information under a false pretense is prohibited. Splash pages, phishing forms, email distribution, proxy email or any relation to phishing activities will result in immediate removal in addition to CenturyLink's other enforcement rights described in this AUP.

- Running any process that sniffs traffic on a network port or otherwise captures traffic not specifically intended for that server, unless explicit authorization is obtained in advance from CenturyLink.
- Operating an account on behalf of, or in connection with, or reselling any service to, persons or firms listed in the Spamhaus Register of Known Spam Operations (ROKSO) database at www.spamhaus.org.

Internet Etiquette: Each Customer is expected to execute reasonable Internet etiquette. The Customer will comply with the rules appropriate to any network to which CenturyLink may provide access. Except as set forth in a services agreement between CenturyLink and Customer, Customer should not post, transmit, or permit Internet access to information the Customer desires to keep confidential. The Customer is not permitted to post any material that is illegal, libelous and tortious, indecently depicts children or is likely to result in retaliation against CenturyLink by offended users.

Cryptocurrency Mining: Any use of digital assets utilizing cryptography or similar computational processing to mine or create units of cryptocurrency, including but not limited to Bitcoin, Ethereum, Ripple, Litecoin, etc., is prohibited.

Illegal Use: Any use of CenturyLink's Services in a manner which is defined or deemed to be statutorily illegal is a direct violation this AUP. This includes, but is not limited to: death threats, terroristic threats, threats of harm to another individual, multi-level marketing schemes, HYIP or Ponzi schemes, invasion of privacy, credit card fraud, racketeering, defamation, slander, and other common illegal activities.

Child Pornography: CenturyLink has a zero tolerance policy on child pornography and related sites and will cooperate fully with any criminal investigation into a Customer's violation of the Child Protection Act of 1984, or any other applicable law.

Terrorist Websites: CenturyLink prohibits the use of its Services for the hosting of terrorist-related web sites. This includes sites advocating human violence and hate crimes based upon religion, ethnicity, or country of origin.

Email Policy

Mass Mailings: CenturyLink has a zero tolerance policy on SPAM, Junk E-mail or UCE. Spam, Junk-mail and UCE are defined as: the sending of the same, or substantially similar, unsolicited electronic mail messages, whether commercial or not, to more than one recipient. A message is considered unsolicited if it is posted in violation of a newsgroup charter or if it is sent to a recipient who has not requested or invited the message. UCE also includes e-mail with forged headers, compromised mail server relays, and false contact information. This prohibition extends to the sending of unsolicited mass mailings from another service, which in any way implicates the use of CenturyLink whether or not the message actually originated from our servers.

Mailing Lists: CenturyLink's mass mailing rules also apply to mailing lists, list servs or mailing services Customer may contract with. An acceptable mailing list will be focused at a targeted audience that has voluntarily signed up for e-mail information or that has made their e-mail address available for distribution of information from Customer. The list must also allow for automatic removal by all end Customers upon request with non-distribution in the future.

If Customer's actions have caused CenturyLink mail servers or CenturyLink IP address ranges to be placed on black hole lists and other mail filtering software systems used by companies on the Internet, in addition to any other enforcement rights of CenturyLink under this AUP, Customer may be assessed a US $500 charge to their account and US $300 per hour for administrative charges incurred to remove and protect mail servers and IP ranges.

In addition to CenturyLink's other enforcement rights set forth in this AUP, violation of the above email policy may result in one or all of the following:

- A warning via email.
- Removal of DNS for the advertised/originating site.
- Temporary shutdown of the server or a block on outgoing mail.
- IP address routing to null.

Repeat violation of the above terms may result in one or more of the following actions:

- Immediate disconnection of service with no re-connection.

- US $500 fee assessed to Customer account for violation.

Intellectual Property Infringement: CenturyLink services may only be used for lawful purposes. Transmission, distribution, or storage of any information, data or material in violation of United States or state regulation or law, or by the common law, is prohibited. This includes, but is not limited to, material protected by copyright, trademark, trade secret, or other intellectual property rights. CenturyLink will cooperate with all law enforcement agencies in relation to alleged intellectual property infringement housed on CenturyLink's services, Website, or servers.

IP Allocation: CenturyLink owns and manages all Internet Protocol (IP) Addresses. IP Addresses are non-transferable from CenturyLink and Customer retains no ownership or transfer rights. All IP Addresses are assigned by the CenturyLink engineering team on a per VLAN, per server basis. Attempted use of IP addresses not originally allocated for use or IP address use on non-assigned VLANs or servers is a violation of this AUP. All IP Addresses are currently registered to CenturyLink via Arin.net assignments or from premier providers that CenturyLink works directly with. Private IP assignments are available to qualified Customers. Use of an IP address in an unauthorized manner may result in a charge of $25 per IP in addition to any other enforcement rights of CenturyLink under this AUP. Use of an IP address in an unauthorized manner that creates a third party Customer outage may result in a US $500 charge and termination of service until the IP allocation issue is resolved, in addition to any other enforcement rights of CenturyLink under this AUP.

Reporting Violation of the Acceptable Use Policy:
CenturyLink accepts reports of alleged violations of this AUP via email sent to abuse@ctl.io. Reports of alleged violations must be verified and must include the name and contact information of the complaining party, and the IP address or website allegedly in violation, and description of the violation. CenturyLink owes no duty to third parties reporting alleged violations but will review all verified third party reports and will take appropriate actions as described below or within its sole discretion.

Enforcement of this AUP: CenturyLink reserves the right, but does not assume the obligation, to strictly enforce this AUP. CenturyLink will use reasonable care in notifying the Customer and in resolving the problem in a method resulting in the least

amount of service interference as reasonably possible. For violations of the AUP, or at CenturyLink's discretion, to prevent a violation of the AUP, CenturyLink reserves the right to:

- Issue warnings;
- Ask the Customer to increase resources;
- Limit Customer access to Services or implement service and resource usage restrictions;
- Assess the applicable fees as set forth in this AUP;
- Suspend Services without notice for any violation of the AUP; and/or
- Terminate Service without notice for a single or for continued and repeated violations of the AUP.

CenturyLink shall be the sole determiner of which of the above actions is to be taken, and can reverse or revise its decision at any time.

back to top

If you have questions about our legal policies, SLA, or to report abuse, please use our contact form.